NMCI Contract N00024-00-D-6000
Awarded 6 October 2000

Attachment 2A
Service Level Agreements

Table of Contents

SERVICE NAME: END-USER PROBLEM RESOLUTION	SLA: 101

Service Description: Problem Resolution of an individual incident is the Contractor-provided service for resolving "trouble calls" reported to the NMCI Help Desk. This problem resolution SLAPC measures the percentage of all resolved NMCI incidents against identified performance target values. This SLAPC applies to both the unclassified and classified NMCI environments.

Performance Category: End User Problem Resolution	Increment 1 SLAPC: 101

Problem Resolution time starts with the opening of a Help Desk incident ticket by the Contractor following receipt of an incident notification. Problem Resolution time stops upon successful resolution of the incident, or when an incident is determined, by pre-agreed Government-Contractor criteria, to fall outside the scope of Contractor responsibility (e.g., transfer of legacy application incidents to appropriate non-NMCI agency, NMCI-to-outside-NMCI interoperability reporting). The Problem Resolution time may pause during a period when Government support is required but not available, such as:

a) Customer, upon proper notification, not available to provide complete information or to continue troubleshooting.

b) Facility not accessible to support problem resolution activities when pre-coordinated (w/ specific start & stop times) with Government. Contractor must demonstrate lack of access was caused by a Government fault and that the problem couldn't be resolved without access.

c) Time required for completion of Government administrative actions (e.g., missing, lost, or stolen equipment).

All measurements are based on a 24 hours a day/7 days a week operation.

Measurement CONOPS:

This SLAPC is the measure of resolution of issues called or emailed in to the NMCI Help Desk and encompasses all customer-facing tickets that are not measured in any other SLAPC specific metric. The measure is based on the difference between the Create Date/Time of the Remedy (help desk ticketing) system and the Resolved Date/Time of the same ticket, minus any time during which the customer is needed but not available to assist in troubleshooting.

On a monthly basis, all customer-facing incident tickets, which were closed in the given reporting month, will be collected and assessed for SLAPC reporting purposes. Those tickets that have been categorized with a Category/Type/Item combination that relates to SLAPC 101, End User Problem Resolution, will be reviewed based on the field titled Total Time Open in Seconds. This field represents all work time associated with the ticket and will have excluded any time the ticket was pending input from the customer.

The following will be excluded from measurement:

- Incidents covered under SLAPC 102, SLAPC 103.6, and SLAPC 105.

Who: Contractor	**Frequency:** Monthly
Where: **User Population:** All Navy; All USMC – Measured separately **Sample Size:** All Tickets	**How Measured (i.e., captured):** End User Incident Reports to Help Desk **Measurement Formula:** Number of closed incidents completed within the required time interval / (Total number of closed incidents) **Frequency of Measure:** Continuous

<table>
<tr><td>Sample Unit:
Closed External Incident Ticket

Where Measured:
Help Desk Trouble Ticket System</td><td colspan="3">Weighting (as applicable):
Equal weighting for all incidents</td></tr>
<tr><td>Aggregation of Data:</td><td colspan="3">Performance data for sites that have not yet achieved Full Performance will be aggregated at the site level and the SLAPC targets will apply at the site level.
Performance data for sites that have achieved Full Performance will be aggregated at the user population level and the SLAPC targets will apply at the user population level.</td></tr>
<tr><td>SLAPC Success Criteria</td><td colspan="3">All targets for each LOS must be met to pass the SLAPC for that LOS.</td></tr>
<tr><td></td><td>Level of Service</td><td>Time Interval</td><td>Percentage Complete</td></tr>
<tr><td rowspan="5">SLAPC Target</td><td rowspan="3">LOS (1 and 2)</td><td><= 4.00 hrs</td><td>>= 80.00%</td></tr>
<tr><td><= 96.0 hrs</td><td>>= 90.00%</td></tr>
<tr><td><= 336 hrs</td><td>>= 99.00%</td></tr>
<tr><td rowspan="2">LOS (3)</td><td><= 2.00 hrs</td><td>>= 90.00%</td></tr>
<tr><td><= 24.0 hrs</td><td>>= 99.00%</td></tr>
</table>

SERVICE NAME: NETWORK PROBLEM RESOLUTION	SLA: 102

Service Description: This SLA measures the resolution of problems associated with the Contractor provided network devices and connections. Network incidents affect multiple users and consequently require a response commensurate with the impact. For example, incidents attributed to a large site, which would impact a higher number of users, and incidents at a *Small Site* with mission critical users as defined below, will be given a more stringent target to meet. This SLA applies to both the unclassified and classified NMCI environments.

Performance Category: Network Problem Resolution	Increment 1 SLAPC: 102

Performance Category Description:
This SLAPC is measured against *validated* network incidents. A network incident is defined as the time during which the customer cannot use network transport services due to a network device failure directly attributable to the Contractor. An incident begins when trouble is detected and reported or a trouble ticket is opened. Time ends when the incident is resolved.

The Government and Contractor have agreed to analyze the target in Jan 2005, and upon mutual agreement readjust the target if deemed necessary

For the purposes of this SLAPC, the following definitions are applicable:

- **Type 1.1 Large Site -** a site that has 250 or more seats.

- **Type 1.2 Small Site -** a site that has between 24-249* seats.
  Note: A small site that has ten (10) or more NMCI mission critical (i.e. CLIN 0008AA or CLIN 0008AB upgrades) seats permanently assigned and installed will be treated as a *Large Site* for SLAPC reporting. (*A limited number of very small sites, as part of the initial rollout, were implemented with the Small Site architecture prior to development of the VSSD architecture. These sites, as well as Type 2 connected sites, shall be included in the Small Site calculation.)

- **Type 2** VSS sites service 23 or fewer seats, and obtain connectivity to the NMCI network for unclassified service via an alternative broadband technology that utilize dedicated/reserved/committed bandwidth for WAN transport to NMCI.

- **Type 3** sites utilizing very small site design (VSSD) network architecture. Type 3 VSSD sites service 23 or fewer seats, have a VSS transport boundary and obtain connectivity to the NMCI network for unclassified service via an alternative broadband technology that does not utilize dedicated/reserved/committed bandwidth for WAN transport to NMCI.

Network Problem Resolution measures the elapsed time from the beginning of the incident until network connectivity is restored. Problem Resolution time *starts* with the opening of a *validated* network incident ticket following receipt of an incident notification (from either an end-user or the network management system (NMS)). *Validated* network problems are those that are confirmed to be network device related. Problem Resolution time *stops* upon successful resolution of the incident. Resolution times will be reported in Remedy tickets.

Additional definitions in regards to this network SLAPC:

External Networks – Those external network devices provided as part of the basic service DISN (NIPRNET and SIPRNET), MCTN, IT-21, and Internet and other networks as specified in attachment 10.

Network Device - the supporting physical hardware, firmware, and software (e.g., switches, routers,

cable plant, boundary equipment, and network uninterruptible power supplies [UPS]) extending from the wall plug to the NOC.

Wide Area Network (***WAN)*** - the Contractor or DISA 'cloud' or backbone and the tail-circuits that connect the 'cloud' to a site's outer router.

Boundary - the information assurance and network devices between the site's outer router and inner router that are required for network connectivity. Types of boundaries implemented on NMCI include:

- Transport Boundary- Logical boundary between the NMCI BAN/LAN and the WAN connectivity circuit provided by one or more of the selected WAN service providers.
- B1- Physical boundary between NMCI and external networks used for transport, e.g., NIPRNET and the USMC COI.
- B2- Physical boundary between NMCI and customer users/applications located within Navy and Marine Corp non-NMCI legacy networks.
- B3-Logical boundary between the NMCI Communities of Interest (COIs).

Base Area Network (***BAN)*** - the devices and cable plant used to connect a site's inner router through the core, distribution layer (when implemented) and to the access layer.

Local Area Network (LAN) - the access layer through to the user wall plug, including cable plant.

Information assurance (IA) equipment includes Virtual Private Network (VPN) devices, boundary firewalls and load balancers.

All measurements are based on a 24 hours a day/7 days a week operation.

Measurement CONOPS:
The measure is based on the difference between the Create Date/Time of the Remedy (help desk ticketing) system and the Resolved Date/Time of the same ticket, minus any time during which the customer is needed but not available to assist in troubleshooting.

On a monthly basis, all Network Problem Resolution customer-facing tickets, which were closed in the given reporting month, will be collected and assessed for SLAPC reporting purposes. Those tickets that have been categorized with a Category/Type/Item combination that relates to SLAPC 102, Network Problem Resolution, will be reviewed based on the field titled Total Time Open in Seconds. This field represents all work time associated with the ticket and will have excluded any time the ticket was pending input from the customer. The Total Time Open in Seconds fields will be combined and divided by the total number of tickets being considered.

Tickets in Resolved status that have not been closed will be considered open tickets.

The following will be excluded from measurement:

- Incidents that result only in the loss of redundancy are not considered in this measure.
- Incidents attributed to the external side of the NMCI demarcation interface of NMCI connections to External Networks will be excluded from this measure.
- Incidents covered under SLAPC 101, SLAPC103.6 and SLAPC 105
- Time required obtaining a VPN PKI server certificate from the Government's Local Registration Authority (LRA).

Who: Contractor	**Frequency:** Monthly
Where:	**How Measured (i.e., captured):** End-user Incident Calls to Help Desk or by tickets opened by NOC

<table>
<tr><td>User Population:
All Navy; All USMC – Measured separately

Sample Size:
All Tickets

Sample Unit:
Open and Closed External Incident Tickets

Where Measured:
Help Desk Trouble Ticket System</td><td colspan="3">Staff when the Network Management System (NMS) detects a network incident

Measurement Formula:
Number of closed incidents completed within the required time interval / (Total number of incidents that are open longer than the required time interval plus all of the closed incidents)

Frequency of Measure:
Continuous

Weighting (as applicable):
Equal weighting for all incidents</td></tr>
<tr><td>Aggregation of Data:</td><td colspan="3">Performance data for sites that have not yet achieved Full Performance will be aggregated at the site level. For these sites, the Contractor may exclude 1 trouble ticket per site, as long as the duration of that trouble ticket does not exceed 22.00 hours duration for Type 1.1 and 1.2 Sites or 30.00 hours duration for Type 2 or 48.00 hours for Type 3 Sites at the site level. The SLAPC target will apply at the site level.

Performance data for sites that have achieved Full Performance will be aggregated at the user population level and the SLAPC target will apply at the user population level.</td></tr>
<tr><td>SLAPC Success Criteria</td><td colspan="3">All targets must be met to pass the SLAPC.</td></tr>
<tr><td rowspan="10">SLAPC Target</td><td>Type of Site</td><td>Time Interval</td><td>Percentage Complete</td></tr>
<tr><td rowspan="3">Type 1.1 - Large Sites</td><td><= 1.00 hr</td><td>>= 25.00%</td></tr>
<tr><td><= 4.00 hrs</td><td>>= 75.00%</td></tr>
<tr><td><= 18.0 hrs</td><td>>= 98.00%*</td></tr>
<tr><td rowspan="2">Type 1.2 - Small Sites</td><td><= 4.00 hrs</td><td>>= 70.00%</td></tr>
<tr><td><= 24.0 hrs</td><td>>= 98.00%*</td></tr>
<tr><td rowspan="2">Type 2 Sites</td><td><= 4.00 hrs</td><td>>= 70.00%</td></tr>
<tr><td><= 24.0 hrs</td><td>>= 98.00%*</td></tr>
<tr><td rowspan="2">Type 3 VSS Sites</td><td><= 12.0 hrs</td><td>>= 80.00%</td></tr>
<tr><td><= 24.0 hrs</td><td>>= 95.00%**</td></tr>
<tr><td colspan="3">* 2% (** or 5% for Very Small Sites) of validated incidents (rounded up to the nearest whole number) include any allowance for ‘outliers’. A small site that has more than ten (10) NMCI mission critical (i.e., CLIN 0008AA or CLIN 0008AB) seats permanently assigned and installed will be treated as a Large Site for SLAPC reporting.</td></tr>
</table>

SERVICE NAME: END-USER SERVICES	SLA: 103

Service Description: End-User Services are the Contractor-provided services that most directly affect the end user. These services E-mail, Web and Portal, File Share, Print, Network Logon, Access to Government Applications, and RAS services. The requirements defined in the End-User Services SLAPC apply to both the unclassified and classified NMCI environments. Resultant measures shall be reported separately for each environment. The End User Services requirements apply to both the unclassified and classified NMCI environments.

Performance Category: E-mail Services - User E-mail Availability	Increment 2 SLAPC: 103.1.1

Performance Category Description: E-mail is the Contractor provided user service for sending and receiving E-mail and attachments. This SLAPC applies to a network-connected NMCI workstation at a Government site, and the shared network storage assigned to that site. This SLAPC excludes RAS and web-based activities.

> **103.1.1 E-mail Services - User E-mail Availability (Increment 2):** Percentage of time E-mail service is available at the end-user workstation. User E-mail Availability is measured by synthetic E-mail transaction generated from the end user workstation across the full connection path of the network infrastructure, to include the user LAN, Base Area Network, WAN, and Server Farm connectivity. A small site sampling is used and the measured performance is assumed to be representative of all users at that site.

The transactions conducted for User E-mail Availability are conducted using synthetic scripts that replicate the actions of a standard E-mail. The intent of these measures is to verify that the supporting NMCI networks, domain name server, directory, security boundaries, E-mail servers, remote procedure calls, and E-mail applications are available and functioning satisfactorily. End-to-End measurement will be a representative sampling of local, regional, and enterprise infrastructure performance.

The Contractor has notified the Government that automated synthetic transactions will not be available until the 1st Quarter calendar year 2005 timeframe incident to the NMCI upgrade to Microsoft Server 2003. Until synthetic transaction measurements are available, User Email Availability will rely on existing E-mail Availability and Performance measures defined in Attachment 2B, Transition Service Level Agreements. These improved measures using automated synthetic transactions (vice manual methods) are a priority for the Government. Upon availability, the Government and Contractor shall, within six months, revise the measurement CONOPs and SLAPC targets.

User E-mail Availability is measured by sampling. For E-mail Availability, all sites with 24 or greater NMCI seats will be configured and conduct synthetic transactions from at least two on-site representative point to ensure reportable data from at least one on-site representative point. If the site receives service from multiple servers than each probe will test a different server. Sites with fewer than 24 NMCI seats will not be measured unless mutually determined by the Government and the Contractor.

For E-mail Availability the Government will approve the location of the measurement points.

Who: Contractor	**Frequency:** Monthly
Where: **User Population:** All Navy; All USMC (measure separately) **Sample Size:** • Sites>=24 seats will have at least two on-site representative points • Sites<24 seats will not be measured unless mutually	**How Measured (i.e., captured):** With an automated tool. **Measurement Formula:** For sites that have not achieved full performance: Total available minutes derived from the representative point on an end-user workstation at the site/ Total minutes in the month For sites that have achieved full performance: Sum of (Total available minutes derived from the representative point on an end-user workstation at the site x number of seats at the site)/ Sum of

determined by Government and Contractor **Sample Unit:** Client **Where Measured:** Client (representative of site)	the seats at all sites **Frequency of Measure:** (goal 5 min) TBD **Weighting (as applicable):** Weighted Average (by seat count)	
Aggregation of Data:	Performance data for sites that have not yet achieved Full Performance will be aggregated at the site level and the SLAPC targets will apply at the site level. Performance data for sites that have achieved Full Performance will be aggregated at the user population level and the SLAPC targets will apply at the user population level.	
SLAPC Success Criteria	All targets must be met, to pass the SLAPC	
SLAPC Target	**User E-mail Availability**	(goal >= 99.7%) TBD

Performance Category: E-mail Services - E-Mail End-to-End (Client-Server-Server-Client Performance	**Increment 2 SLAPC: 103.1.2**
Performance Category Description: E-mail is the Contractor provided user service for sending and receiving E-mail and attachments. This SLAPC applies to a network-connected NMCI workstation at a Government site, and the shared network storage assigned to that site. This SLAPC excludes RAS and web-based activities. **103.1.2 E-mail Services - E-Mail End-to-End (Client-Server-Server-Client) Performance (Increment 2):** Percentage of synthetic E-mail and 10K attachment transactions successfully processed and returned in the required time, stated in minutes roundtrip. Transactions are generated at the client, processed by the host server, forwarded to an appropriate NMCI destination server, responded to via an auto-reply generated by the destination server, and returned to the client. The transactions conducted for End-to-End performances are conducted using synthetic scripts that replicate the actions of a standard E-mail. The intent of these measures is to verify that the supporting NMCI networks, domain name server, directory, security boundaries, E-mail servers, remote procedure calls, and E-mail applications are available and functioning satisfactorily. End-to-End measurement will be a representative sampling of local, regional, and enterprise infrastructure performance. The Contractor has notified the Government that automated synthetic transactions will not be available until the 1st Quarter calendar year 2005 timeframe incident to the NMCI upgrade to Microsoft Server 2003. Until synthetic transaction measurements are available, End-to-End Performance will rely on existing E-mail Availability and Performance measures defined in Attachment 2B, Transition Service Level Agreements. These improved measures using automated synthetic transactions (vice manual methods) are a priority for the Government. Upon availability, the Government and Contractor shall, within six months, revise the measurement CONOPs and SLAPC targets to incorporate the defined automated synthetic transactions described above. For E-Mail End-to-End Performance, the Government will approve the location of the measurement points. End-to-end performance will utilize the actual value received or (TBD goal 30 minutes) for any failed test without an associated network or server availability outage documented in another SLA measurement.	
Measurement CONOPS: TBD	
Who: Contractor	**Frequency:** Monthly
Where: **User Population:** All Navy; All USMC (measured separately) **Sample Size:** TBD **Sample Unit:** Client **Where Measured:** Client (representative of site)	**How Measured (i.e., captured):** With an automated tool **Measurement Formula**: Number of attempts successful within the required Time Interval / Total number of attempts **Frequency of Measure:** (goal 5 min) TBD **Weighting (as applicable):** Weighted Average (by seat count)
Aggregation of Data:	Performance data for sites that have not yet achieved Full Performance will be aggregated at the site level and the SLAPC targets will apply at the site level. Performance data for sites that have achieved Full Performance will be aggregated at the user population level and the SLAPC targets will apply at the user population level.
SLAPC Success Criteria	All targets must be met, to pass the SLAPC

SLAPC Target	E-Mail End-to-End Performance	Time Interval	Percentage Complete
		(goal <= 5.00 min) TBD	(goal >= 95.0%) TBD
		(goal <= 10.00 min) TBD	(goal >= 99.5%) TBD

Performance Category: E-mail Services - E-Mail Server Service Availability	**Increment 1 SLAPC: 103.1.3**

Performance Category Description: E-mail is the Contractor provided user service for sending and receiving E-mail and attachments. This SLAPC applies to a network-connected NMCI workstation at a Government site, and the shared network storage assigned to that site. This SLAPC excludes RAS and web-based activities.

> **103.1.3 E-mail Services - E-Mail Server Service Availability (Increment 1):** Percentage of time the Mail Transfer Service at the E-mail server is online, running, and the Mail Queue is processing or available for processing mail. The terms "active" and "processing" are defined to mean that NMCI user-generated E-mail is capable of or is being received and delivered. Server Service Availability is measured at every E-mail "service" at the Server Farm. The term "service" indicates that there may be more than one server identified for processing E-mail for a given user, and availability of any one meets the requirement for the associated set of users.

Measurement CONOPS:
All E-mail servers are monitored by Tivoli TEC. If there is an outage, a TEC event will be detected and a Remedy ticket will be created with the start time of the event.

On a monthly basis, all E-mail Server Service customer-impacting tickets, which were closed in the given reporting month, will be collected and assessed for SLAPC reporting purposes. Those tickets that have been categorized with a Category/Type/Item combination that relates to this SLAPC will be reviewed based on the field titled Total Time Open in Seconds. This field represents all work time associated with the ticket and will have excluded any time the ticket was pending due to input/access needed from customer. The Total Time Open in Seconds fields will be combined and calculation will be performed.

The following will be excluded from measurement:

- Non-active servers (e.g., backup servers in server clusters) do not count if multiple servers provide the service.

Who: Contractor	**Frequency:** Monthly
Where: **User Population:** All Navy; All USMC (measured separately) **Sample Size:** All servers **Sample Unit:** Server **Where Measured:** Server	**How Measured (i.e., captured):** With an automated tool and end user trouble calls to Help Desk **Measurement Formula:** For sites that have not achieved full performance:: Total available minutes of active email servers at the server farm/ Total minutes in the month x total number of email servers at the server farm For sites that have achieved full performance: Total available minutes of active email servers / Total minutes in the month x total number of email servers at the server farm **Frequency of Measure:** Continuous **Weighting (as applicable):** Equal Weighting

Aggregation of Data:	Performance data for sites that have not yet achieved Full Performance will be aggregated at the site level and the SLAPC targets will apply at the site level. Sites shall inherit the performance level of the email servers that provide the service to them. Performance data for sites that have achieved Full Performance will be aggregated at the user population level and the SLAPC targets will apply at the user population level.	
SLAPC Success Criteria	All targets must be met, to pass the SLAPC	
SLAPC Target	**Server Service Availability**	>= 99.70%

Performance Category: E-mail Services - E-mail Client Responsiveness	**Increment 2 SLAPC: 103.1.4**

Performance Category Description: E-mail is the Contractor provided user service for sending and receiving E-mail and attachments. This SLAPC applies to a network-connected NMCI workstation at a Government site, and the shared network storage assigned to that site. This SLAPC excludes RAS and web-based activities.

> **103.1.4 E-mail Services - E-Mail Client Responsiveness (Increment 2):** Percentage of transactions sent by the users that fall within the response time to successfully open an e-mail with a 10K attachment. This measure provides a host server response time to an end user initiated request and is measured at the NMCI user workstation.

The transactions conducted for Client Responsiveness are conducted using synthetic scripts that replicate the actions of a standard E-mail. The intent of these measures is to verify that the supporting NMCI networks, domain name server, directory, security boundaries, E-mail servers, remote procedure calls, and E-mail applications are available and functioning satisfactorily. End-to-End measurement will be a representative sampling of local, regional, and enterprise infrastructure performance.

The Contractor has notified the Government that automated synthetic transactions will not be available until the 1st Quarter calendar year 2005 timeframe incident to the NMCI upgrade to Microsoft Server 2003. Until synthetic transaction measurements are available, E-mail Client Responsiveness will rely on existing E-mail Availability and Performance measures defined in Attachment 2B, Transition Service Level Agreements. These improved measures using automated synthetic transactions (vice manual methods) are a priority for the Government. Upon availability, the Government and Contractor shall, within six months, revise the measurement CONOPs and SLAPC targets to incorporate the four defined automated synthetic transactions described above.

E-mail Client Responsiveness is measured by sampling. All sites with 24 or greater NMCI seats will be configured and conduct synthetic transactions from at least two on-site representative points to ensure reportable data from at least one on-site representative point. If the site receives service from multiple servers than each probe will test a different server.

E-mail Client responsiveness will utilize the actual value received for any failed test without an associated network or server availability outage documented in another SLAPC measurement. The Contractor can select the best response from any of the site probes for any particular time measurement to account for individual seat issues, the expressed intent is to ensure the availability of an appropriate measurement for each time interval at each site.

For Client Responsiveness, the Government will approve the location of the measurement points.

End-to-end performance will utilize the actual value received or (TBD goal 30 minutes) for any failed test without an associated network or server availability outage documented in another SLA measurement.

Measurement CONOPS:
All E-mail servers are monitored by Tivoli TEC. If there is an outage, a TEC event will be detected and a Remedy ticket will be created with the start time of the event.

On a monthly basis, all E-mail Server Service customer-impacting tickets, which were closed in the given reporting month, will be collected and assessed for SLAPC reporting purposes. Those tickets that have been categorized with a Category/Type/Item combination that relates to SLAPC 103.1.3, E-mail Server Service, will be reviewed based on the field titled Total Time Open in Seconds. This field represents all work time associated with the ticket and will have excluded any time the ticket was pending due to input/access needed from customer. The Total Time Open in Seconds fields will be combined and calculation will be performed. The following will be excluded from measurement:

- Non-active servers (e.g., backup servers in server clusters) do not count if multiple servers provide the service.

Who: Contractor	**Frequency:** Monthly

<table>
<tr><td>Where:

User Population:
All Navy; All USMC (measured separately)

Sample Size:

- Sites>=24seats will have at least two on-site representative points
- Sites<24 seats will not be measured unless mutually determined by Government and Contractor

Sample Unit:
Client

Where Measured:
Client (representative of site)</td><td colspan="3">How Measured (i.e., captured):
With an automated tool.

Measurement Formula:
Number of attempts successful within the required Time Interval / Total number of attempts

Frequency of Measure:
(goal 5 min) TBD

Weighting (as applicable):
Weighted Average (by seat count)</td></tr>
<tr><td>Aggregation of Data:</td><td colspan="3">Performance data for sites that have not yet achieved Full Performance will be aggregated at the site level and the SLAPC targets will apply at the site level.

Performance data for sites that have achieved Full Performance will be aggregated at the user population level and the SLAPC targets will apply at the user population level.</td></tr>
<tr><td>SLAPC Success Criteria</td><td colspan="3">All targets must be met, to pass the SLAPC</td></tr>
<tr><td rowspan="3">SLAPC Target</td><td rowspan="3">Client Responsiveness</td><td>Time Interval</td><td>Percentage Complete</td></tr>
<tr><td>(goal <= 2.00 sec) TBD</td><td>(goal >= 95.0%) TBD</td></tr>
<tr><td>(goal <= 4.00 sec) TBD</td><td>(goal >= 99.5%) TBD</td></tr>
</table>

Performance Category: Web and Portal Services	**Increment 2** **SLAPC: 103.2**

Performance Category Description: Web and Portal Services are the Contractor provided services that allow end users to access web content as supported by the NMCI network. This SLAPC applies to web/portal services obtained through an NMCI network-connected NMCI user workstation and excludes services obtained through RAS. The performance measure for Web Services is End-to-End Performance.

> **End-to-End Performance:** Percentage of synthetic web transactions successfully processed and returned in the required time (i.e., Time Interval (*x*) seconds roundtrip). Web-access transactions are generated at the NMCI client, processed through the NMCI network (including PKI infrastructure), resulting in an authenticated website displayed on the NMCI client internet browser.
>
> The measurement of end-to-end performance will include validation of:
> - Supporting PKI services (excludes initial authentication of a DoD PKI certificate)
> - A representative PKI-enabled, NMCI-hosted static website
> - A B1 and/or B1 DMZ security suite
> - Supporting Domain Name Services

The intent of this measure is to provide indication of the performance of the end-to-end set of service components required for the end-user to access Contractor-hosted web and portal services located in the NMCI DMZ. It is targeted at providing indication of the services obtained from the network operations center (NOC) where the B1 and NMCI portal are located.

The transactions for Web and Portal Services End-to-End performance, are conducted using synthetic scripts that replicate the actions of a web request. The intent of the measures is to verify that the supporting NMCI networks, domain name server, directory, security boundaries, web servers, remote procedure calls is available and functioning satisfactorily. End-to-End measurement will be a representative sampling of local, regional, and enterprise infrastructure performance.

The Contractor has notified the Government that automated synthetic transactions will not be available until the 1st Quarter calendar year 2005 timeframe incident to the NMCI upgrade to Microsoft Server 2003. Until synthetic transaction measurements are available, the defined Web and Portal measurement -- End-to-End Performance will rely on existing Web Access Services Availability and Performance measures defined in Attachment 2B, Transition Service Level Agreements. These improved measures using automated synthetic transactions (vice manual methods) are a priority for the Government. Upon availability, the Government and Contractor shall, within six months, revise the measurement CONOPs and SLAPC targets to incorporate the defined automated synthetic transactions described above.

All sites with 24 or greater NMCI seats selected for sampling will be configured and conduct synthetic transactions from at least two on-site representative points to ensure reportable data from at least one on-site representative point. Each probe will test a different server. Client responsiveness will utilize the actual value received or (TBD goal 30 sec) seconds for any failed test without an associated network or server availability outage documented in another SLAPC measurement. The Contractor can select the best response from any of the probes at a given site for any particular time measurement to account for individual seat issues, the expressed intent is to ensure the availability of an appropriate measurement for each time interval at each site sampled.

For End-to-End Performance, the Government will approve the location of the measurement points.

Measurement CONOPS: TBD	
Who: Contractor	**Frequency:** Monthly
Where: **User Population:** All Navy; All USMC (measured separately)	**How Measured (i.e., captured):** Automated tool **Measurement Formula:** Number of attempts successful within the required time interval / Total

<table>
<tr><td>Sample Size:
TBD

Sample Unit:
Client

Where Measured:
Measured at all sites using a representative NMCI client workstation to a B1 DMZ web server</td><td colspan="3">number of attempts

Frequency of Measure:
TBD

Weighting (as applicable):
Equal weighting for all sites.</td></tr>
<tr><td>Aggregation of Data:</td><td colspan="3">Performance data for sites that have not yet achieved Full Performance will be aggregated at the site level and the SLAPC targets will apply at the site level.

Performance data for sites that have achieved Full Performance will be aggregated at the user population level and the SLAPC targets will apply at the user population level.</td></tr>
<tr><td>SLAPC Success Criteria</td><td colspan="3">All target s must be met to pass the SLAPC</td></tr>
<tr><td rowspan="3">SLAPC Target</td><td rowspan="3"><u>End-to-End Performance</u></td><td>Time Interval (x)</td><td>% Complete</td></tr>
<tr><td>(goal <= 5.00 sec) TBD</td><td>(goal >= 95.0%) TBD</td></tr>
<tr><td>(goal <= 8.00 sec) TBD</td><td>(goal >= 99.8%) TBD</td></tr>
</table>

Performance Category: File Share Services – Server Availability	**Increment 1 SLAPC: 103.3.1**
Performance Category Description: File Share Services is the Contractor provided service that allows NMCI end users to store and retrieve files on shared, controlled access storage media. This SLAPC applies to a network-connected NMCI user, at his/her assigned normal Government workstation site, and the shared network storage assigned to that site. The performance measures for File Shared Services are Server Availability and Client Responsiveness. **103.3.1 Server Availability:** Percentage of time the end user's File Share Service is active and available for transfer. Server Availability is measured at every File Share server. The availability measure does not include any supporting network infrastructure. Note: Server Availability for file share is not an end-to-end measure and depends on the companion SLAPC for E-mail to provide indication of the availability of the intervening user to server end-to-end availability.	
Measurement CONOPS: All file servers are monitored using Tivoli TEC. If there is an outage, a TEC event will be detected and a Remedy ticket will be created with the start time of the event. On a monthly basis, all File Server Availability customer-impacting tickets, which were closed in the given reporting month, will be collected and assessed for SLAPC reporting purposes. Those tickets that have been categorized with a Category/Type/Item combination that relates to SLAPC 103.3.1, File Server Availability, will be reviewed based on the field titled Total Time Open in Seconds. This field represents all work time associated with the ticket and will have excluded any time the ticket was pending due to input/access needed from customer. The Total Time Open in Seconds fields will be combined and calculation will be performed.	
Who: Contractor	**Frequency:** Monthly
Where: **User Population:** All Navy; All USMC (measured separately) **Sample Size:** All servers **Sample Unit:** File Share Server **Where Measured:** Server	**How Measured (i.e., captured):** Automated tool and end user calls to Help Desk **Measurement Formula:** For sites that have not achieved full performance: Total available minutes of file share servers at the server farm/ Total minutes in the month x total number of file share servers For sites that have achieved full performance: Total available minutes of file share servers / Total minutes in the month x total number of file share servers **Frequency of Measure:** Continuous **Weighting (as applicable):** Equal weighting
Aggregation of Data:	Sites that have not yet achieved Full Performance shall meet the requisite target(s) at the site level. Sites shall inherit the performance level of the file share servers that provide the service to them. Sites having achieved Full Performance will be aggregated at the user population level.
SLAPC Success Criteria	All target levels within each performance measure must be met, to pass the SLAPC.

SLAPC Target	**Server Availability** (for sites that have not achieved full performance)	>= 99.50%
	Server Availability (for aggregation of sites that have achieved full performance)	>= 99.80%

Performance Category: File Share Services – Client Responsiveness	**Increment 1 SLAPC: 103.3.2**

Performance Category Description: File Share Services is the Contractor provided service that allows NMCI end users to store and retrieve files on shared, controlled access storage media. This SLAPC applies to a network-connected NMCI user, at his/her assigned normal Government workstation site, and the shared network storage assigned to that site.

> **103.3.2 File Share Services - Client Responsiveness**: This key SLAPC measures the network responsiveness to the end user by demonstrating the data transfer time of the host server, both to pull a file from the server and to push a file to the server. It is the average time the synthetic file transactions take to successfully transfer a scripted 1MB file between an NMCI File Share server and an NMCI user. Client Responsiveness is measured at the NMCI user workstation.

Client Responsiveness is measured by sampling. All sites with 24 or greater NMCI seats will be configured and conduct synthetic transactions from at least two on-site representative points to ensure reportable data from at least one on-site representative point. If the site receives service from multiple servers than each probe will test a different server. Sites with fewer than 24 seats will not be measured unless mutually determined by the Government and the Contractor.

Client responsiveness will utilize the actual value received or 10 seconds for any failed test without an associated network or server availability outage documented in another SLAPC measurement. The Contractor can select the best response from any of the site probes for any particular time measurement to account for individual seat issues, the expressed intent is to ensure the availability of an appropriate measurement for each time interval at each site.

Measurement CONOPS:
The file transfer tests are performed using a Visual Basic Intrinsic. The shared disk environment is setup prior to starting the measurement timer. A 1-megabyte file of random characters is used for the network-attached test. The 103.3.2 SLAPC measurement of LAN connected workstations copies the 1–megabyte file once every 5 minutes to the fileserver (KAPM_FILECOPYUP). The second part of the test reverses the process and workstation copies the 1-megabyte file from the fileserver to the local disk once every 5 minutes (KAPM_FILECOPYDOWN).

Who: Contractor	**Frequency:** Monthly
Where: **User Population:** All Navy; All USMC (measured separately) **Sample Size:** • Sites >=24seats will have at least two on-site representative points • Sites <24seats will not be measured unless mutually determined by Government and Contractor **Sample Unit:** Client **Where Measured:** Client (Representative of site.)	**How Measured (i.e., captured):** Automated tool **Measurement Formula:** Sum of all non-excluded client responsiveness measured values / Total number of non-excluded attempts **Frequency of Measure:** Client Responsiveness- Every 5 minutes **Weighting (as applicable):** Equal weighting

Aggregation of Data:	Performance data for sites that have not yet achieved Full Performance will be aggregated at the site level and the SLAPC targets will apply at the site level. Sites shall inherit the performance level of the file share servers that provide the service to them. Performance data for sites that have achieved Full Performance will be aggregated at the user population level and the SLAPC targets will apply at the user population level.	
SLAPC Success Criteria	All targets must be met, to pass the SLAPC	
SLAPC Target	**Client Responsiveness**	**Average Time Interval**
		<= 2.00 sec

<table>
<tr><td colspan="2">Performance Category: Print Services</td><td>Increment 1
SLAPC: 103.4</td></tr>
<tr><td colspan="3">Performance Category Description: Print Services is the Contractor provided service that allows end users to produce black & white and color hard copies of electronic documents and transparencies. This SLAPC applies to a network-connected NMCI user, at his/her assigned normal Government workstation site, and the shared network print server assigned to that site. The performance measure for Print Services is Server Availability.

<u>Server Availability:</u> Percentage of time that Print queues are active and available at the Print Server for transferring a print job to a local printer. Server Availability is measured at every Print server.</td></tr>
<tr><td colspan="3">Measurement CONOPS:
All print servers are monitored using Tivoli TEC. If there is an outage, a TEC event will be detected and a Remedy ticket will be created with the start time of the event.

On a monthly basis, all Print Server Availability customer-impacting tickets, which were closed in the given reporting month, will be collected and assessed for SLAPC reporting purposes. Those tickets that have been categorized with a Category/Type/Item combination that relates to this SLAPC, Print Server Availability, will be reviewed based on the field titled Total Time Open in Seconds. This field represents all work time associated with the ticket and will have excluded any time the ticket was pending due to input/access needed from customer. The Total Time Open in Seconds fields will be combined and calculation will be performed.</td></tr>
<tr><td>Who: Contractor</td><td colspan="2">Frequency: Monthly</td></tr>
<tr><td>Where:

User Population:
All Navy; All USMC (measured separately)

Sample Size:
All Servers

Sample Unit:
Print Server

Where Measured:
Server</td><td colspan="2">How Measured (i.e., captured):
Automated tool and end user calls to Help Desk

Measurement Formula:

For sites that have not achieved full performance: Total available minutes of print servers at the server farm/ Total minutes in the month x total number of print servers

For sites that have achieved full performance: Total available minutes of print servers / Total minutes in the month x total number of print servers

Frequency of Measure:
Continuous

Weighting (as applicable):
Equal weighting</td></tr>
<tr><td>Aggregation of Data:</td><td colspan="2">Performance data for sites that have not yet achieved Full Performance will be aggregated at the site level and the SLAPC targets will apply at the site level. Sites shall inherit the performance level of the print servers that provide the service to them.

Performance data for sites that have achieved Full Performance will be aggregated at the user population level and the SLAPC targets will apply at the user population level.</td></tr>
<tr><td>SLAPC Success Criteria</td><td colspan="2">All targets must be met, to pass the SLAPC</td></tr>
<tr><td>SLAPC Target</td><td>Server Availability</td><td>>= 99.50%</td></tr>
</table>

Performance Category: Network PKI Logon Services	**Increment 1** **SLAPC: 103.5**
Performance Category Description: Network PKI Logon Services is the Contractor-provided service for end-user access to the Enterprise Validation Authority (EVA) Server and NMCI Active Directory in support of end-user Public Key Infrastructure (PKI) logon to the NMCI network. This SLAPC excludes logon to the network through RAS and web-based activities. The performance measure for Network Logon Services is Client Responsiveness. **Client Responsiveness:** Percentage of transactions that fall within the response time to successfully complete cryptographic network logon from an NMCI network-attached workstation. The measurement is the time required for the supporting NMCI infrastructure to process the end-user cryptographic log on request. Client Responsiveness shall be measured by sampling. Initial sample size shall consist of 50 measures that provide a representative sampling of the deployed architecture (e.g., Navy and USMC sites, geographic location, local and distant user-to-server farm connections). CONOPs and supporting documentation	
Measurement CONOPS: The measurements are obtained manually by using a stopwatch. After inserting the smart card into the smart card reader and entering the appropriate Personal Identification Number (PIN) number when prompted, the start point for the measurement is the time from when the "Return" key is depressed. The stopping point will be when the screen depicting "Loading your personal settings" is shown on the monitor. Every time measurement is recorded and forwarded to a collection point – to the GIAC SLAPC Collector. All time trials are used to compute the percentage above or below the threshold value. All measurements for this SLAPC will be taken by an EDS administrator and periodically observed by the Government. Test will occur during the morning hours, 0800 – 1000 local. The test will utilize a CAC with minimum 32 KB chip as indicated on the CAC being used.	
Who: Contractor	**Frequency:** Monthly
Where: **User Population:** All Navy; All USMC (measured separately) **Sample Size:** The selection of sites will be mutually agreed to by the Government and Contractor and include 3 large sites (2000+ seats), 4 medium sites (250 – 2000 seats), and 3 small sites (25 – 250 seats). The 10 sites will rotate monthly, with 5 of the 10 sites being replaced with same-sized sites. **Sample Unit:** Test Account at sample site **Where Measured:** NMCI client workstation to EVA Server and Active Directory	**How Measured (i.e., captured):** Stopwatch test at sample sites **Measurement Formula:** Number of attempts successful within the required Time Interval during the test period / Total number of attempts during the test period **Frequency of Measure:** 0800-1000 Local time **Weighting (as applicable):** Equal weighting
Aggregation of Data:	Performance data for sites that have not yet achieved Full Performance will be aggregated at the site level and the SLAPC targets will apply at the site level. Performance data for sites that have achieved Full Performance will be aggregated at the user population level and the SLAPC targets will apply at the user population level.

SLAPC Success Criteria	All targets must be met, to pass the SLAPC		
SLAPC Target	Client Responsiveness	Time Interval	Percentage Complete
		<= 30.0 sec	>= 90.00%

Performance Category: Problem Resolution for Access to Government Applications	**Increment 1 SLAPC: 103.6**

Performance Category Description: Problem Resolution for Access to Government Applications is the Contractor-provided service for end-user access to Government-approved applications. Government-approved applications are defined as applications that are approved by the Government to operate on NMCI and that users are authorized access from within NMCI. Problem Resolution measures the percentage of all resolved access to Government-approved application incidents against SLAPC identified performance target values.

The Problem Resolution time may *pause* during a period when Government support is required but not available, such as:

a) Customer, upon proper notification, is not available to provide complete information or to continue troubleshooting.

b) Facility not accessible to support problem resolution activities when pre-coordinated (w/ specific start & stop times) with Government. Contractor must demonstrate lack of access was caused by a Government fault and that the problem couldn't be resolved without access.

c) Time is required for completion of Government administrative actions (e.g., missing, lost, or stolen equipment).

All measurements are based on a 24 hours a day/7 days a week operation.

Measurement CONOPS:
This SLAPC is the measure of resolution of issues called or emailed in to the NMCI Help Desk and encompasses customer-facing tickets that are associated with accessing Navy, Marine Corp or other DoD applications. The measure is based on the difference between the Create Date/Time of the Remedy (help desk ticketing) system and the Resolved Date/Time of the same ticket, minus any time during which the customer is needed but not available to assist in troubleshooting. It does not include the distribution of new software ordered either via a CLIN or via a Service Request.

On a monthly basis, all customer-facing incident tickets, which were closed in the given reporting month, will be collected and assessed for SLAPC reporting purposes. Those tickets that have been categorized with a Category/Type/Item combination that relates to SLAPC 103.6, Access to Government Applications Problem Resolution, will be reviewed based on the field titled Total Time Open in Seconds. This field represents all work time associated with the ticket and will have excluded any time the ticket was pending input from the customer.

The following will be excluded from measurement:

a) Any Government-directed change to the network that affects accessibility of an application.

Who: Contractor	**Frequency:** Monthly
Where: **User Population:** All Navy; All USMC – Measured separately, by 4-Site Code **Sample Size:** All tickets **Sample Unit:** Closed External Incident Ticket **Where Measured:** Help Desk Trouble Ticket System	**How Measured (i.e., captured):** End user calls to the Help Desk **Measurement Formula:** Number of closed incidents completed within the required time interval / Total number of the closed incidents **Frequency of Measure:** Continuous **Weighting (as applicable):** Equal weighting for all incidents

Aggregation of Data:	Performance data for sites that have not yet achieved Full Performance will be aggregated at the site level and the SLAPC targets will apply at the site level. Performance data for sites that have achieved Full Performance will be aggregated at the user population level and the SLAPC targets will apply at the user population level.		
SLAPC Success Criteria	All targets for each LOS must be met to pass the SLAPC for that LOS.		
SLAPC Target	**Level of Service**	**Time Interval**	**Percentage Complete**
	LOS (1 & 2)	<= 24.0 hrs	>= 85.00%
		<= 96.0 hrs	>= 90.00%
		<= 336 hrs	>= 99.00%
	LOS 3	<= 4.00 hrs	>= 90.00%
		<= 24.0 hrs	>= 98.00%

Performance Category: RAS Services – Service Availability	**Increment 1 SLAPC: 103.7.1**

Performance Category Description: Unclassified RAS (uRAS) is the Contractor-provided service that allows users to remotely and securely connect to the NMCI. A remote NMCI user accesses NMCI by connecting an NMCI laptop to an analog phone line and launching an application to connect to the Contractor Dial Access Network (DAN). The Contractor DAN has filters to route NMCI traffic the uRAS Transport Boundary. The user then launches a VPN application to create a secure data tunnel into NMCI to gain access to NMCI services.

> **103.7.1 RAS Service Availability:** Percentage of time that the uRAS Dial-up Service is active at the NOC and available for access. WAN access circuits at each RAS Access Points are the transport for the NMCI destined traffic once a user successfully connects to the Contractor DAN. The availability measure excludes any supporting network infrastructure not controlled by or contracted for by the NMCI.

For RAS Availability, as long as any one of the test sites in each COI (e.g. one of the RAS Access Points) is meeting the test for that 5 minute test cycle, the test is successful.

Note: All NMCI uRAS modems will operate at the current industry standard connectivity rate, and support automated selection of lower rates based on geographic distance, and modem and line quality. This measurement is based on the use of an industry standard modem -- currently 56Kb/sec.

Measurement CONOPS:

RAS Availability: The KAPM script collects data every 5 minutes; every 6 hours the data is uploaded to an Oracle DB via a Tivoli custom inventory scan.. The data extracted by Business Objects are KAPM probes fired 24 X 7 excluding the hours of 0900, 1900, and 2300 local time when the KAPM probe is used to measure SLAPC 103.7.2.

For the RAS portion of the SLAPC measurement, the connection speed is collected into the MIF file and subsequently into the Oracle database. On the initial release of KAPM, a single UUNET access point number is dialed and left connected. The number is recorded in the MIF file for each measurement and subsequently placed in the Oracle database.

Who: Contractor	**Frequency:** Monthly
Where: **User Population:** All Navy; All USMC – (measured separately). **Sample Size:** One representative user per RAS access point, using a representative standard NMCI laptop, dialing into a local Contractor DAN POP and authenticating with a VPN gateway **Sample Unit:** RAS Access point **Where Measured:** RAS Access Point, or other NMCI Facilities	**How Measured (i.e., captured):** **Measurement Formula:** Total available hours of RAS Connectivity for the test period / (1260 minutes x numbers of days in the month) **Frequency of Measure:** Every 5 Minutes, excluding the hours of 0900, 1900, and 2300 local time when the KAPM probe is used to measure SLAPC 103.7.2. **Weighting (as applicable):** Equal weighting

Aggregation of Data:	Sites will be aggregated at the user population level.	
SLAPC Success Criteria	All targets must be met, to pass the SLAPC	
SLAPC Target	**RAS Service Availability**	>= 99.00%

Performance Category: RAS Services – Client Responsiveness	**Increment 1** **SLAPC: 103.7.2**

Performance Category Description: Unclassified RAS (uRAS) is the Contractor-provided service that allows users to remotely and securely connect to the NMCI. A remote NMCI user accesses NMCI by connecting an NMCI laptop to an analog phone line and launching an application to connect to the Contractor Dial Access Network (DAN). The Contractor DAN has filters to route NMCI traffic the uRAS Transport Boundary. The user then launches a VPN application to create a secure data tunnel into NMCI to gain access to NMCI services.

> **103.7.2 Client Responsiveness:** Percentage of synthetic file transactions that fall within the required response time to successfully transfer a scripted 100KB file between an NMCI File Share server and an NMCI uRAS client. This measurement will be taken during a connection to the Contractor DAN of at least 52.3 Kb/sec. This key SLAPC measures the uRAS responsiveness to the end user by demonstrating the data transfer time of the uRAS connectivity, both to download a file from the server and to upload a file to the server during one session. uRAS Dial-up Client Responsiveness is measured at the representative NMCI user laptop. The measure is structured to factor out the effects of the dial in line.

For RAS Availability, as long as any one of the test sites in each COI (e.g. one of the RAS Access Points) is meeting the test for that 5 minute test cycle, the test is successful.

Note: All NMCI uRAS modems will operate at the current industry standard connectivity rate, and support automated selection of lower rates based on geographic distance, and modem and line quality. This measurement is based on the use of an industry standard modem -- currently 56Kb/sec.

Measurement CONOPS:

The file transfer tests are performed using a Visual Basic Intrinsic. The 103.7.2 SLAPC measurement copies 100 KB file thirty-one times from the local disk to the shared drive from the file server (KAPM_RAS_FILECOPYUP) per hour. The second part of the test reverses the process and thirty-one copies are made from the file server share to the local drive (KAPM_RAS_FILECOPYDOWN) per hour. After the test is complete, the shared disk environment is torn down. The test result is recorded in the MIF file and subsequently into the Oracle database.

Who: Contractor	**Frequency:** Monthly
Where: **User Population:** All Navy; All USMC – (measured separately). **Sample Size:** One representative user per RAS access point, using a representative standard NMCI laptop, dialing into a local Contractor DAN POP and authenticating with a VPN gateway **Sample Unit:** Client **Where Measured:** From the Client to a supporting NMCI File Server not collocated with	**How Measured (i.e., captured):** **Measurement Formula:** Number of attempts successful within the required time interval/ Total number of attempts **Frequency of Measure:** 0900, 1900, 2300 local time, 7 days/week, for one hour each, Thirty-one copies are made from the local disk to the shared drive from the file server. The second part of the test reverses the process and thirty-one copies are made from the file server share to the local drive. **Weighting (as applicable):** Equal weighting

the Service Access Point.				
Aggregation of Data:	Sites will be aggregated at the user population level.			
SLAPC Success Criteria	All targets must be met, to pass the SLAPC			
SLAPC Target	**Client Responsiveness (100KB file transfer)**		**Time Interval**	**Percentage Complete**
		Upload	<= 40.0 sec	>= 90.00%
		Download	<= 22.0 sec	>= 90.00%

<table>
<tr><td colspan="2">Performance Category: Blackberry Services</td><td>Increment 1
SLAPC: 103.8</td></tr>
<tr><td colspan="3">Performance Category Description: An NMCI user equipped with a Blackberry accesses NMCI via a commercial wireless service provider infrastructure. (This access begins at the Blackberry and includes a wireless link to an RF tower and then a terrestrial link via the Internet/NIPRNET to an NMCI access point.) This access is at an NMCI B1 Firewall of a supporting NMCI NOC, to a supporting Blackberry server (a Blackberry Enterprise Server [BES] to which a Blackberry device is assigned). The BES passes the Blackberry E-mail to the correct NMCI Exchange E-mail Server, where it is processed as a normal Exchange E-mail. Based on user attributes in Active Directory, it also replicates the E-mail action on the corresponding Outlook client at the users desktop. In the reverse scenario, there is a re-director at the Outlook client software that cues the system to generate a parallel Email to the BES and out to the Blackberry via the supporting wireless infrastructure.

Availability is supported by a stand-by mirrored back up server.</td></tr>
<tr><td colspan="3">Measurement CONOPS:
All BES servers are monitored using Tivoli TEC. If there is an outage, a TEC event will be detected and a Remedy ticket will be created with the start time of the event.

On a monthly basis, all BES Server/Blackberry Service Availability customer-impacting tickets, which were closed in the given reporting month, will be collected and assessed for SLAPC reporting purposes. Those tickets that have been categorized with a Category/Type/Item combination that relates to SLAPC 103.8, Blackberry Service Availability, will be reviewed based on the field titled Total Time Open in Seconds. This field represents all work time associated with the ticket and will have excluded any time the ticket was pending due to input/access needed from customer. The Total Time Open in Seconds fields will be combined and calculation will be performed.</td></tr>
<tr><td>Who: Contractor</td><td colspan="2">Frequency: Monthly</td></tr>
<tr><td>Where:

User Population:
All Navy; All USMC (measured separately)

Sample Size:
All (100%) BES services

Sample Unit:
BES Servers

Where Measured:
BES Servers</td><td colspan="2">How Measured (i.e., captured):
Automated tool to measure service availability at the BES and user calls to Help Desk

Measurement Formula:
Blackberry Service Availability = Total available hours of Blackberry Service / Total hours in the month

Frequency of Measure:
Continuous

Weighting (as applicable):
Equal weighting</td></tr>
<tr><td>Aggregation of Data:</td><td colspan="2">Sites will be aggregated at the user population level.</td></tr>
<tr><td>SLAPC Success Criteria</td><td colspan="2">All targets must be met, to pass the SLAPC.</td></tr>
<tr><td>SLAPC Target</td><td>Blackberry Service Availability</td><td>>= 99.70%</td></tr>
</table>

SERVICE NAME: HELP DESK	SLA: 104

Service Description: Help Desk Services is the Contractor provided technical support for NMCI end users. The Contractor will be the first point of contact for all authorized NMCI users. Users may interact or communicate with help desk by phone and e-mail. The performance measures for Help Desk Services are: 1) Average Speed of Answer, 2) Average Speed of Response – Voice Mail/E-mail, 3) Call Abandonment Rate, and 4) First Call Resolution. Help Desk requirements apply to both the unclassified and classified NMCI environments.

Performance Category: Average Speed of Answer - Telephone Calls	**Increment 1** **SLAPC: 104.1.1**

Performance Category Description: The Average Speed to Answer (ASA) is the monthly average of the amount of time that a caller will wait, after choosing the last voice menu prompt, before a live agent answers. A customer will be offered the option to leave a voice mail or continue to wait for a live agent. If a customer chooses to leave a voicemail, the amount of time calculated will be the time between choosing the last prompt on the initial voice menu and the time that the customer selects the voicemail option.

Measurement CONOPS:

This SLAPC is the measure of time, following a call to the NMCI Help Desk, between the selection of the last prompt on the Automated Call Distribution (ACD) system [call is considered at this point to be in queue] and the call being answered by a help desk agent, or the user choosing to leave a voicemail. Abandoned calls, either prior to listening to the phone prompts or after selected the last phone prompt will be excluded from this calculation. Calls will not be segmented by seat type nor by prime time vs. non-prime time.

On a monthly basis, the summary field in the ACD system that is titled ANSTIME will be added to the summary field in the ACD system that is titled OUTFLOWTIME. These two fields represent the total number of seconds associated with calls waiting in the queue and the queue time for calls that go to voicemail, respectively. The sum of these two figures is divided by the total calls offered to the queue minus any abandoned calls. This value is the average speed to answer.

Who: Contractor	**Frequency**: Monthly	
Where: **User Population:** All DON **Sample Size:** All calls **Sample Unit:** End User calls to Help Desk **Where Measured:** Help Desk automated call distribution system	**How Measured (i.e., captured):** End user calls to the Help Desk **Measurement Formula:** Total number of seconds from the last voice menu prompt until a live agent answers for all answered calls to Help Desk / Total number of calls answered by Help Desk **Frequency of Measure:** Continuous **Weighting (as applicable):** Equal weighting for all calls	
Aggregation of Data:	Sites will be aggregated at the user population level.	
SLAPC Success Criteria	All targets must be met, to pass the SLAPC	
SLAPC Target	**Average Speed to Answer**	<= 40.0 seconds

<table>
<tr><td colspan="2">Performance Category: Average Speed of Response – Voice Mail/E-mail</td><td>Increment 2
SLAPC: 104.1.2</td></tr>
<tr><td colspan="3">Performance Category Description: If a customer elects to leave a voice mail or e-mail message with the help desk instead of speaking with a live agent, the help desk will contact the customer regarding the voice mail or e-mail. The customer must provide in the voice mail or e-mail accurate contact information (i.e., name and phone number). The receipt time/date stamp of the voice mail or e-mail will be the start time; the creation of the trouble ticket with e-mail or voice reply will end the SLAPC measurement.

The Contractor has notified the Government that the required technology is not currently available. Upon availability of the technology, the Government and the Contractor shall, within six months develop the measurement CONOPs and SLAPC targets to implement this SLAPC.</td></tr>
<tr><td colspan="3">Measurement CONOPS: TBD</td></tr>
<tr><td>Who: Contractor</td><td colspan="2">Frequency: Monthly</td></tr>
<tr><td>Where:

User Population:
All DON

Sample Size:
All calls and emails

Sample Unit:
End user calls and emails to Help Desk

Where Measured:
Help Desk Trouble Ticket System</td><td colspan="2">How Measured (i.e., captured):
End user calls and emails sent to the Help Desk

Measurement Formula:
Voice Mail = Total response time (in minutes) of all Voice Mail tickets / Total number of Voice Mail tickets

E-mail = Total response time (in hours) of all E-mail tickets / Total number of E-mail tickets

Frequency of Measure:
TBD

Weighting (as applicable):
Equal weighting for all responses. Both performance elements must be separately passed in order to meet the SLAPC performance.</td></tr>
<tr><td>Aggregation of Data:</td><td colspan="2">Sites will be aggregated at the user population level.</td></tr>
<tr><td>SLAPC Success Criteria</td><td colspan="2">All targets must be met, to pass the SLAPC</td></tr>
<tr><td rowspan="2">SLAPC Target</td><td>Average Speed of Response Voice mail</td><td>(goal 60.00 min) TBD</td></tr>
<tr><td>Average Speed of Response E-mail</td><td>(goal 4.00 hrs) TBD</td></tr>
</table>

Performance Category: Call Abandonment Rate	**Increment 1 SLAPC: 104.2**

Performance Category Description: The Call Abandonment Rate is the percentage of calls that are terminated by the customer following the selection of the last voice menu prompt and prior to a live agent answering the call.

Measurement CONOPS:

Call abandonment rate is measured against phone calls placed by NMCI users to the NMCI help desk and received by the automated call distribution system (ACD).

For the purposes of this SLA, an NMCI user is identified as a caller who selects all of the ACD menu prompts applicable to their problem type. Callers that select the final ACD menu prompt are placed in the ACD queue and offered the opportunity to communicate with the Help Desk. Their calls are then characterized as offered in one of the following three ways:

1. NMCI Users in queue may wait for a live Help Desk agent to answer and handle their call.
2. NMCI Users in queue may choose to be transferred to Voice Mail that will then handle their call.
3. NMCI Users in queue may abandon the call either before a live agent answers or they choose to transfer to Voice Mail. These calls are not handled.

Callers that hang up before the final ACD menu prompt are not included in the abandonment calculation.

Who: Contractor	**Frequency:** Monthly	
Where: **User Population:** All DON **Sample Size:** All calls **Sample Unit:** End user calls to the Help Desk **Where Measured:** Automated Call Distribution System	**How Measured (i.e., captured):** End user calls to the Help Desk **Measurement Formula:** Number of calls abandoned / Offered calls **Frequency of Measure:** Continuous **Weighting (as applicable):** Equal weighting for all abandoned calls	
Aggregation of Data:	Sites will be aggregated at the user population level.	
SLAPC Success Criteria	All targets must be met, to pass the SLAPC	
SLAPC Target	**Call Abandonment Rate**	<= 5.00%

Performance Category: First Call Resolution	**Increment 1 SLAPC: 104.3**

Performance Category Description: The percentage of answered calls to the help desk that are resolved on the initial call in the following scenarios:

a) Problems and/or issues resolved within 30.0 minutes of the initial call to the Help Desk while the user remains on the phone line.
b) Problems and/or issues resolved within 30.0 minutes of a return call to the customer from a Help Desk agent in response to an e-mail/voicemail.
c) Problems and/or issues resolved within 30.0 minutes of the initial call by the NOC or other Help Desk Subject Matter Expert due to a warm transfer, which results in problem being resolved while the user remains on the phone line.
d) Cases in which the end user is redirected to another support center outside NMCI (e.g., Government or Commercial Legacy Application Help Desk), after determining that responsibility for resolution lies outside of NMCI.

Measurement CONOPS:
This SLAPC is the percentage of tickets called or emailed into the NMCI Help Desk that were resolved on the first contact with the help desk agent. The 30.0minute time measure is based on the difference between the Create Date/Time of the Remedy (help desk ticketing) system and the Resolved Date/Time of the same ticket.

On a monthly basis, all customer-facing tickets, which were closed in the given reporting month will be collected and assessed for SLAPC reporting purposes. Those tickets that have been resolved by the Help Desk or Network Operation Center (NOC), will be reviewed based on the field titled Total Time Open in Seconds. This field represents all work time associated with the ticket and will have excluded any time the ticket was pending input from the customer. The field First_Call_Resolution is then reviewed. The number of tickets that have "Yes" in the First_Call_Resolution field is divided by the total number of tickets resolved by the Help Desk and NOC.

Who: Contractor	**Frequency:** Monthly	
Where: **User Population:** All Navy; All USMC – Measured Separately **Sample Size:** All tickets **Sample Unit:** Closed External Incident Ticket **Where Measured:** Help Desk Trouble Ticket System	**How Measured (i.e., captured):** End user incident reports to the Help Desk **Measurement Formula:** For all closed tickets during the reporting period, The number of tickets resolved* on the first call / Closed tickets *"tickets resolved" must meet Description criteria (a-d) above. **Frequency of Measure:** Continuous **Weighting (as applicable):** Equal weighting for all calls	
Aggregation of Data:	Sites will be aggregated at the user population level.	
SLAPC Success Criteria	All targets for each LOS must be met to pass the SLAPC for that LOS.	
SLAPC Target	**Level of Service**	**Percentage Complete**
	LOS 1 & 2	>= 65.00%
	LOS 3	>= 80.00%

SERVICE NAME: MOVE, ADD, CHANGE	SLA: 105

Service Description: The Contractor-provided service for moves, adds and changes as specified in the Statement of Objectives. This SLAPC applies equally to software updates and other actions taken by the Contractor as part of normal network/systems administration. (See SOO 3.1.13) This SLAPC measures the time to complete MAC activity, from the receipt of the MAC request from an authorized Government submitter to the completion of the MAC activity. MAC requirements apply to both the unclassified and classified NMCI environments.

Performance Category: Move, Add, Change	Increment 1 SLAPC: 105

Performance Category Description: MAC time starts with the Contractor's receipt of an approved MAC request from an authorized submitter. The time of completion of this activity stops upon successful completion of the MAC. The MAC time may pause during a period when Government support is required but not available, such as:

a) Incomplete information in the MAC request.

b) Customer not available to schedule an appointment.

c) Customer not available for scheduled appointment.

d) Facility not available for access to perform MAC.

e) Time required for security certifications and accreditation.

f) Authorized rescheduling by the Government end-user or authorized submitter.

g) Other category exceptions as approved by the PCO.

All measurements are based on a 24 hours a day/7 days a week operation.

Measurement CONOPS:
This SLAPC is the measure of resolution of Move, Add, Changes (MAC) into the NMCI Help Desk and encompasses all customer-facing change requests that are defined as MACs. The measure is based on the difference between the Requested Service Date of the Remedy (help desk ticketing) system and the Resolved Date/Time of the same ticket, minus any time during which the customer is needed but not available to assist in troubleshooting.

On a monthly basis, all customer-facing change requests, which were closed in the given reporting month, will be collected and assessed for SLAPC reporting purposes. Those change requests that have been categorized with a Category/Type/Item combination that relates to SLAPC 105, Move, Add, Change, will be reviewed based on the field titled Total Time Open in Seconds. This field represents all work time associated with the change request and will have excluded any time the ticket was pending input from the customer. The Total Time Open in Seconds fields will be reviewed. The total change requests for each of the timeframes will be divided by the total change requests being considered.

Who: Contractor	**Frequency:** Monthly
Where: **User Population:** All Navy & All USMC – Measured separately **Sample Size:** All requests **Sample Unit:**	**How Measured (i.e., captured):** **Measurement Formula:** Short Term MAC Delivery Performance = MACs completed within short term target in month / Total MACs completed in month *Where the numerator of the equation is:* MACs completed within short term target in a month = (# Level of Services (1) & (2) MACS <= 24.0 hrs) + (# Level of

<table>
<tr><td>MAC change requests

Where Measured:
Service Request Management and Help Desk ticketing systems</td><td colspan="2">Service (3) MACS < 4.00 hours))

<u>Mid Term MAC Delivery Performance</u> = MACs completed within mid term target in month / Total MACs completed in month

Where the numerator of the equation is:
MACs completed within mid term target in a month = (#Level of Services (1) & (2) MACS < 96.0 hrs) + (#Level of Service (3) MACS Level of Service (3) < 48.0 hrs))

Frequency of Measure:
Continuous

Weighting (as applicable):
Equal weighting.</td></tr>
<tr><td>Aggregation of Data:</td><td colspan="2">Performance data for sites that have not yet achieved Full Performance will be aggregated at the site level and the SLAPC targets will apply at the site level.

Performance data for sites that have achieved Full Performance will be aggregated at the user population level and the SLAPC targets will apply at the user population level.</td></tr>
<tr><td>SLAPC Success Criteria:</td><td colspan="2">All targets must be met, to pass the SLAPC</td></tr>
<tr><td rowspan="3">SLAPC Target</td><td>Type</td><td>Percentage Met</td></tr>
<tr><td>Short Term MAC Delivery Performance</td><td>>= 85.00%</td></tr>
<tr><td>Mid Term MAC Delivery Performance</td><td>>= 96.00%</td></tr>
</table>

SERVICE NAME: INFORMATION ASSURANCE SERVICES	SLA: 106

Service Description: Information Assurance (IA) Services provide protection of the Information Infrastructure and Systems, Domains and Communities of interest, and Content (at rest, in-use and in-transit) in order to assure confidentiality, integrity, availability, authenticity, and non-repudiation. The Contractor is required to provision security mechanisms, procedures, controls and operations in compliance with DOD and DON policy and guidance. The NMCI IA service shall also be in compliance with DoD certification and accreditation policies and procedures. The performance categories for IA services are: 1) Security Event Detection, 2) Security Event Reporting, 3) Security Event Response, and 4) IA Configuration Management.

A computer security event is any observable occurrence in a system or network. Events include, for example, a user connecting to a file share, a server receiving a request for a Web page, a user ending sending electronic mail (e-mail), and a firewall blocking a connection attempt. An *NMCI reportable event* is an event with a potentially negative consequence, such as unauthorized system access, system crash, network packet flood, unauthorized use of system privileges, defacement of a Web page, or the execution of malicious code that destroys data. All categories of incidents (provided in Appendix A) are considered to be NMCI reportable events.

For the purposes of this SLAPC, the term "security event" will be synonymous with "NMCI reportable event."

This SLA applies to both the unclassified and classified NMCI environments.

Performance Category: Security Event Detection	Increment 1 SLAPC: 106.1

Performance Category Description: Security Event Detection is defined as the capability required to detect security events as specified by JTF-CNO and summarized in the Detection and Reporting Category Matrix (DRCM) [Appendix A to this SLAPC]. The Government will instantiate these requirements through Red and Green Team test cases (provided in the Information Assurance Performance Baseline [IAPB] (Revision 1 of 22 September 04) and maintained in the Red Team Test Procedure Guide. Modifications to test cases will be in accordance with Section 6.10 (c) of the conformed contract.

A "detected event" is one where the Contractor recognizes that "event" and reports the event to the GNOC or records the discovery of the event in a non-perishable "auditable" log.

For an event to be categorized as "detected," the Contractor must present evidence (e.g., security event logs, event reports to GNOC) that the Contractor discovered the event and recognized it as such within one hour of event cessation.

An "auditable log" is a file where entries are made in real-time; where the identity and location of the person making the entry is captured and recorded; where the time of the entry is automatically recorded and is verifiable; and whose entries cannot be altered or repudiated.

The Contractor, upon request, may audit Red Team test procedures and results.

Measurement CONOPS:

NETWARCOM/MCNOSC appointed Red Teams will conduct security test events per the IAPB and the Red Team Test Procedure Guide (see "Exclusions"). Reported results will include, for example, date/time/location of successful attempt and whatever other specific data the Contractor requires to perform root cause or audit results.

All security events will be treated as real world. A final report will be issues to the PCO by the 15th day of the month following the test month. The NETWARCOM/MCNOSC appointed Red Teams will provide a list of Red Team initiated events to be used as the basis for the "Number of Red Team initiated events" in the measurement formula. For the purposes of "Security Event Detection" only, access attempts that originate from outside the NMCI enclave will not be considered in the calculation of this SLAPC if:

1) those attempts/probes are blocked by the outer router/firewall, and

2) the access attempt is unsuccessful, and

3) the attempt does not constitute a denial of service attack.

Successful penetrations from outside the NMCI enclave *will* be included in calculating this SLAPC value.

The following will be excluded from measurement:

1. The Red Team test cases 6-02C, 6-02U, 6-04C, and 6-04U will commence in February 2005.

2. Any relaxation of Government-directed detection requirements must be by Contractor written request, be positively endorsed by the Marine Corps and Navy DAAs, and concurred with by STRATCOM, JTF-CNO, and/or DISA.

Who: Government	**Frequency:** Monthly
Where: **User Population:** All Navy; All USMC (measured separately) • A failed site will not be retested the month following its failure. • Up to 20% of cutover NMCI sites will be tested annually during build-out. • 10% of all NMCI sites will be tested annually . once 75% of the sites have attained full performance. **Sample Size:** Minimum of 100 Red Team initiated security events per month in each Navy and USMC enterprise. **Sample Unit:** Security events as described in the DRCM Appendix A. **Where Measured:** Information from all sources will be considered: e.g., GIAC/RIAC/IAC/NOC/GNOC/EMF watches, IDS Logs, Audit Logs, Trouble Tickets, Incident Reports, and External Sources. The Contractor must present evidence that indicates the security administrator identified and recognized the event within one hour of event cessation.	**How Measured (i.e., captured):** Red Team will note the start/stop time of the event. This time will be compared with the time of detection. **Measurement Formula:** Number of Red Team initiated security event detections / Number of Red Team initiated security events **Frequency of Measure:** Per NMCI reportable event **Weighting (as applicable):** Equal weighting for all units.
Aggregation of Data:	**Sites will be aggregated at the user population level.**
SLAPC Success Criteria	All targets must be met, to pass the SLAPC.

SLAPC Target	**Priority * Level**	**% Attained**
	Serious	>= 95.00%
	Significant	>= 85.00%
	Simple**	>= 75.00%
	* Priority levels per the DRCM (Appendix A). ** Incident Categories 5 and 7 only.	

<table>
<tr><td colspan="3">Performance Category: Security Event Reporting</td><td colspan="2">Increment 1
SLAPC: 106.2</td></tr>
<tr><td colspan="5">Performance Category Description: Security Event Reporting is defined as the time required for the Contractor, upon detection of an adverse security event, to report the security event to the GNOC/MCNOSC. Reportable Security events are specified by JTF-CNO and described in the CND DRCM (Appendix A to this SLAPC), IAPB, and SSAA.

For the purposes of this SLAPC only, Category 3 and Category 6 events (see Appendix A) that originate from outside the NMCI enclave are not considered reportable if those attempts/probes are properly blocked by the outer router/firewall and do not constitute a denial of service attack.

Any relaxation of Government-directed time requirements must be by Contractor written request and be approved by the Navy DAA and Marine Corps DAA.</td></tr>
<tr><td colspan="5">Measurement CONOPS: In accordance with IAPB approved test cases.</td></tr>
<tr><td colspan="2">Who: Government</td><td colspan="3">Frequency: Monthly</td></tr>
<tr><td colspan="2">Where:

User Population:
All Navy; All USMC (measured separately)

Sample Size:
All (100%) of detections of Red Team initiated security events.

Sample Unit:
Security event Reports to CND Service Providers (NAVCIRT and MARCERT) (Contractor reports directly to Navy NNSOC or USMC MCNOSC respectively)

Where Measured:
a) NAVCIRT and MARCERT Telephonic, Electronic and written Logs

b) Contractor GIAC/GNOC telephonic, electronic and written logs, Remedy tickets, or e-mails.

c) Results of “Security Event Detection” performance category of this SLAPC.</td><td colspan="3">How Measured (i.e., captured):
a) Post event report analysis will be conducted by Navy and/or Marine Corps Government Red Teams.

b) Red Team initiated events will be measured from time of detection (as reported in the previous performance category) to submission of report to GNOC or MCNOSC.

Measurement Formula:
The number of security events detected and reported within the required timeframes/ The total number of security events detected.

Frequency of Measure:
Per NMCI reportable event

Weighting (as applicable):
Equal weighting for all units.</td></tr>
<tr><td colspan="2">Aggregation of Data:</td><td colspan="3">Sites will be aggregated at the user population level.</td></tr>
<tr><td colspan="2">SLAPC Success Criteria</td><td colspan="3">All targets must be met, to pass the SLAPC</td></tr>
<tr><td rowspan="4">SLAPC Target</td><td>Priority * Level</td><td>Reporting Time</td><td colspan="2">Percentage Attained</td></tr>
<tr><td>Serious</td><td><= 15.0 min</td><td colspan="2">>= 95.00 %</td></tr>
<tr><td>Significant</td><td><= 120 min</td><td colspan="2">>= 85.00 %</td></tr>
<tr><td>Simple</td><td><= 24.0 hrs</td><td colspan="2">>= 75.00 %</td></tr>
<tr><td colspan="2"></td><td colspan="3">* Priority levels per the DRCM (Appendix A).</td></tr>
</table>

Performance Category: Security Event Response	Increment 1 SLAPC: 106.3

Performance Category Description: Security Event Response is defined as the Contractor's ability to effectively respond to a security event. This incorporates Pre-Planed Responses, Routine Responses, and Urgent Responses as specified in the Incident Response Plan maintained by the Contractor and approved by the DAAs. "Effective response" is defined as being able to attain a specific end state within a specified period of time.

Upon reporting of a security event, action is taken to determine the scope and minimize the effects of the event, restore any lost capability and prevent similar events from happening in the future. Actions should be consistent with the Incident Response Plan, however, only the end state is measured. The desired end state and time frame will vary depending on the type of security event (see table). Only Red Team initiated security events reported by the Contractor and for which permission to respond has been granted by NNSOC or MCNOSC will be considered in the scoring. Timeframe is measured from time NNSOC or MCNOSC gives Contractor permission to respond to time end state is attained. Each eligible security event will be assessed a PASS or FAIL.

Event Type	Desired End State	Measurement
Unauthorized Scanning	Scanning blocked/removal of offending machine (logically)removed from network. Contractor will coordinate physical removal, as appropriate, with NNSOC or MCNOSC, but time to physical remove a workstation will not be measured in the performance category. (Note: this test must be held in abeyance until IDS' realignment occurs.	Logical Removal: 60.0 minutes after receiving direction from the governing authority (NNSOC or MCNOSC).
Rogue machine on network	Rogue machines logically removed from the network upon detection. Contractor will coordinate physical removal, as appropriate, with NNSOC or MCNOSC, but time to physical remove a workstation will not be measured in the performance category.	Logical Removal: 60.0 minutes after receiving direction from the governing authority (NNSOC or MCNOSC).
Unauthorized software (Hacker tool) on network	Disabled user account and offending workstation logically removed from the network. Contractor will coordinate physical removal, as appropriate, with NNSOC or MCNOSC, but time to physical remove a workstation will not be measured in the performance category. (During Increment 1, response only applies to non-NIDS related testing.)	Logical Removal and lock out user account: 60.0 minutes after receiving direction from the governing authority (NNSOC or MCNOSC).
Malicious Insider activity	Logically removed from the network. Contractor will coordinate physical removal, as appropriate, with NNSOC or MCNOSC, but time to physical remove a workstation will not be measured in the performance category. (During	Logical Removal and lock out user account: 60.0 minutes after receiving direction from the governing authority (NNSOC or MCNOSC).

	Increment 1, response only applies to non-NIDS related testing.)	
Unauthorized personnel in EDS controlled areas	Personnel in the custody of Government or EDS personnel.	5.00 minutes after being identified as unauthorized personnel.

Note: Following the completion of this test, and when requested by the Red Team lead, the disabled Red team accounts will be re-enabled to allow for further testing.

Measurement CONOPS:
EDS will report to Government when desired end state is attained. Red Team will compare Red Team logs with GNOC and EDS logs report to verify timeframe for desired end state. All security events will be treated as real world events, even if created by Government Test Teams. Only Red Team initiated security events will be included in the calculation for this SLAPC.

Government-directed timeframes provided with IAVAs, CTOs, INFOCON levels, etc., will take precedence.

Who: Contractor	**Frequency:** Monthly
Where: **User Population:** All Navy; All USMC (measured separately) **Sample Size:** All Contractor-reported Red Team security events where authority to respond has been given by the governing authority (NNSOC or MCNOSC). **Sample Unit:** Reported security event.	**How Measured (i.e., captured):** Watch logs, GNOC logs, Red Team logs, Incident reports. **Measurement Formula:** Total number of detected Red Team events completed in required timeframes / Total number of detected Red Team events. **Frequency of Measure:** Per NMCI reportable event **Weighting (as applicable):** Equal weighting for all units.
Aggregation of Data:	**Sites will be aggregated at the user population level.**
SLAPC Success Criteria	All targets must be met, to pass the SLAPC
SLAPC Target	>= 95.00%

Performance Category: Configuration Management	**Increment 1 SLAPC: 106.4**

Performance Category Description: IA Configuration Management measures the Contractor's ability to remotely maintain NMCI critical component configurations and to correctly apply upgrades, patches, settings, and INFOCON levels. The basis for security configuration is the NMCI Contract, the signed SSAA and as approved through the current IATO as issued by the Operational Commander DAAs.

The component configuration includes the overall software stack installed on the machines including, but not limited to, operating systems, middleware or application software, versions and patch levels, IA/CND/Security applications, and schema information for all relevant IA components.

Any relaxation of Government-directed IA confirmation requirements must be by Contractor written request and approved by the Navy/Marine Corps DAA.

"Correction Time" begins when the Government notifies (via email) the Contractor of the test results. Notification e-mail must include details of all found discrepancies on all system components tested.

Measurement CONOPS: In accordance with IAPB approved test cases

The following will be excluded from measurement:

- Verifiable user actions or inactions (e.g., not connecting to the network during updates) that prevent patches or policies from being applied, and thus impact the ability for NMCI user workstations to be compliant with security policy.
- Verifiable NMCI components (e.g., servers supporting GOTS applications) configured differently for valid operational commander DAA approved reasons. These differences will be maintained in configuration management and tested to this approved IA configuration standard using the above requirements.
- Deployed workstations (when disconnected from NMCI), S&T workstations and developmental workstations.

Who: Government	**Frequency:** Monthly
Where: **User Population:** All Navy; All USMC (measured separately) **Sample Size:** a. No more than 25,000 workstations tested in a given month. b. Minimum of 20% of sites per service per calendar year. The Government will provide the Contractor the list of sites scheduled for testing no less than 45 days in advance. **Sample Unit:** Hardware Components and critical designated components, to include boundary components, servers and workstations. Designated components as described in the NMCI Contract and SSAA.	**How Measured (i.e., captured):** a. Government Green Team will perform a 1st Pass automated scan of the specified IA components. b. Contractor must meet the 1st Pass values specified in the tables above. c. The Contractor, upon Government notification, will generate an End-User Problem Resolution trouble ticket within 48.0 hours and correct the configurations for the components that failed the scans within the Correction Times specified. d. Government will then rescan the failed components identified during the 1st Pass to determine if they are in compliance. The overall score per category must meet or exceed the second pass requirement. In the case of workstations, the Contractor is required to meet a 90.00% overall score on the second pass. e. The tracking and oversight of the components still not repaired after the second pass will shift to the problem resolution Service Level Agreement. f. A hardware component (includes the overall software stack installed on the machines including, but not limited to, operating systems, middleware or application software, versions and patch levels, IA/CND/Security applications, and schema information for all relevant IA components) with one

		or more security misconfiguration represents a failed component **Measurement Formula:** Service Level Attained = Number of properly configured Contractor managed NMCI components / Total number of Contractor managed components tested		
Aggregation of Data:		**Sites will be aggregated at the user population level.**		
SLAPC Success Criteria (Unclassified)		• This SLAPC shall be considered failed if the first pass percentage is not met on the first pass scan. • To meet the category level requirement, the overall score per category must meet or exceed the second pass requirement. • All three categories levels have to be met to pass the SLAPC.		
SLAPC Success Criteria (Classified)		• This SLAPC shall be considered failed if the first pass percentage is not met on the first pass scan. • To meet the category level requirement, the overall score per category must meet or exceed the second pass requirement. • All three categories levels have to be met to pass the SLAPC.		
SLAPC Target Classified: SIPRNET	**Category Level**	**1**	**2**	**3**
	1st Pass % Attained	>= 99.00%	>= 98.00%	>= 80.00%
	Correction Time	12.0 hrs	48.0 hrs	120 hrs
	2nd Pass % Attained	= 100.0%	= 100.0%	>= 90.00%
SLAPC Target Unclassified: NIPRNET	**Category Level**	**1**	**2**	**3**
	1st Pass % Attained	>= 99.00%	>= 96.00%	>= 80.00%
	Correction Time	12.0 hrs	72.0 hrs	168 hrs
	2nd Pass % Attained	= 100.0%	>= 99.00%	>= 90.00%
		Priority components are defined as follows: • Category 1 – Boundary Components (e.g., firewalls, transport boundary devices, VPNs, Ors) • Category 2 – Servers and internal networking devices • Category 3 – Workstations		

SERVICE NAME: NMCI INTRANET	SLA: 107

Service Description: The NMCI Intranet is the trusted network, provided as part of the NMCI service contract, which resides inside the NMCI Boundary 1 Firewalls. The NMCI Intranet interconnects the Navy and Marine Corps bases, server farms, and Network Operation Centers (NOCs). The Intranet extends to the external edge (inner routers) of bases served by NMCI and provides the single transport for the integrated service supporting voice, video or data (as appropriate). The performance measures for this SLAPC are Availability, Latency/Packet Loss, and Quality of Service (QoS) in support of Video Teleconferencing and Voice-over-IP. These measures apply to all NMCI sites regardless of user population. This SLA applies to both the unclassified and classified NMCI environments.

Performance Category: Availability	Increment 1 SLAPC: 107.1

Performance Category Description: NMCI Intranet Availability measure includes the bases served by NMCI, the NMCI NOCs, and the Server Farms (to be called a site). Availability is measured by site, from one NMCI site point of presence – across the tail circuit, across the NMCI backbone, across another tail circuit – to another NMCI site point of presence, and includes any successful* connection path across the network infrastructure. The point of presence is considered to be an inner router (either of the inner routers where a site is configured with redundant routers). Weighting of availability at a site is factored into the measurement and is directly related to the number of NMCI user seats at a site.

*"Successful" is defined as the ability to transfer an ICMP packet from the source to the target and receive a response from the target.

In January 2005, the Government and Contractor will analyze the target and upon mutual agreement readjust the target if deemed necessary.

Measurement CONOPS:
SLAPC 107.1 is measured via the Network Management System's (NMS) Tivoli NetView solution, which is installed at a Network Operation Center (NOC). NetView issues an Internet Control Message Protocol (ICMP)"ping" to each inner router at every site connected to each NOC. The response to the ping indicates connectivity to the site exists.

The solution involves the following:

NetView initiates a 64-byte ping, which is similar to a small data file, and receives a reply. This ability to send a file and receive a response indicates the Intranet is available. The measurement is continuous where the ping is automatically sent every five (5) minutes.

1. NetView captures a "node down" event from the inner router when there is no response to the ping thereby indicating an Intranet outage.
2. When either the device or WAN becomes available, a "node up" event is generated and captured in NetView. The elapsed time between "down" and "up" events is used to compute the elapsed time of the outage for the availability SLA.

NetView stores event data in a file named *trapd.log*. After the file size reaches eight (8) megabytes, a script exports the file to the SLAPC Oracle database. At the end of the day, another script exports the day's final file to one database table. Within the database, the raw data is aggregated and calculated for SLAPC reporting by executing a Perl script daily. Crystal Reports would be used to produce final SLAPC reports with results by site along with enterprise availability.

SLAPC Target adjustment for DISN Performance:

- The DISN core (backbone) is allocated availability of 99.95% corresponding to 21.60 minutes per month of outage.
- If the DISN core (backbone) performance during a month can be shown through documented evidence to exceed 21.60 minutes of outage time, then the SLAPC Targets for that month shall be adjusted by the difference between the actual DISN core (backbone) outage time and 21.60 minutes.

<table>
<tr><td>Who: Contractor</td><td colspan="2">Frequency: Monthly</td></tr>
<tr><td>Where:

User Population:
All Navy; All USMC – (measured separately)

Sample Size:
All sites

Sample Unit:
Inner router at each site

Where Measured:
Measured at the inner router at a site transport boundary. Where there are multiple routers at a transport boundary, only one must have operating connectivity to meet this requirement.</td><td colspan="2">How Measured (i.e., captured):
Automated tool

Measurement Formula:
<u>Site Availability</u> = (Total minutes in a month – Total outage time for a site) / Total minutes in the month

<u>NMCI Availability</u> = (SUM OF (Site Availability for each site x Total number of seats at that site)) / Sum of the seats at all sites

Frequency of Measure:
Every 5 minutes

Weighting (as applicable):
Weighted Average (by seat count)</td></tr>
<tr><td>Aggregation of Data:</td><td colspan="2">Performance data for sites that have not yet achieved Full Performance will be aggregated at the site level and the SLAPC targets will apply at the site level.

Performance data for sites that have achieved Full Performance will be aggregated at the user population level and the SLAPC targets will apply at the user population level.</td></tr>
<tr><td>SLAPC Success Criteria</td><td colspan="2">All targets must be met, to pass the SLAPC</td></tr>
<tr><td rowspan="4">SLAPC Target</td><td>Type of site</td><td>Target</td></tr>
<tr><td>Type 1*</td><td>99.80%</td></tr>
<tr><td>Type 2**</td><td>99.75%</td></tr>
<tr><td>Type 3***</td><td>99.50%</td></tr>
</table>

- Type 1*: All sites with the exception of types below

- Type 2**: sites that service 23 or fewer seats, and obtain connectivity to the NMCI network for unclassified service via an alternative broadband technology that utilizes dedicated/reserved/committed bandwidth for WAN transport to NMCI.

- Type 3***: sites utilizing very small site design (VSSD) network architecture

Note: Type 3 VSSD sites service 23 or fewer seats, have a VSS transport boundary and obtain connectivity to the NMCI network for unclassified service via an alternative broadband technology that does not utilize dedicated/reserved/committed bandwidth for WAN transport to NMCI.

The type 2 and 3 values shall be adjusted, as appropriate, based on actual performance data from 40 VSSD sites, of which 20 sites shall be Marine Corps sites. An attempt shall be made to select sites that comprise a representative sample of the technology solutions under consideration. If Marine Corps site implementation is delayed, performance shall be evaluated using the Navy site data and re-evaluated once Marine Corp performance data is available.

Performance Category: Latency/Packet Loss	Increment 1 SLAPC: 107.2

Performance Category Description:

Latency provides an indicator of the efficiency of the NMCI Intranet. It indicates the time it takes an IP packet to transit between selected NMCI site pairs, measured by roundtrip time.

Packet loss is the percentage of packets lost in transit between the inside interface of selected NMCI inner router pairs. Packet Loss is a strong indicator of the WAN Transport capacity versus loading and provides a measure of the level of contention that data packets encounter as they transit the Intranet.

While Intranet availability is measured at all NMCI sites, latency and packet loss are measured only at Government-Contractor agreed upon site pairs. Latency measurements will be representative samplings of local, regional, and enterprise infrastructure performance. The Contractor will instrument and collect data for a minimum of 100 agreed-to pairs. The Government and Contractor will mutually agree to adjust the site pairs when/if required, with the intent of quantifying performance where sub-optimum service is experienced. Approximate distances must be maintained during any subsequent pair changes in order to meet the requirement values (because of distance dependency). Site pairs will include both classified and unclassified network services.

For the small sites utilizing the very small site design (VSSD) architecture, latency and packet loss measurements will be taken from the transport boundary inner router of the server farm to which the site is homed to the sites' virtual private network (VPN) device. Data will be collected and measured for 20 sample sites, 10 for Navy and 10 for USMC.

Type 3 VSSD sites service 23 or fewer seats, have a VSS transport boundary and obtain connectivity to the NMCI network for unclassified service via an alternative broadband technology such as xDSL, , cable modem, or internet fractional T-1 as specified within the original design document approved by the Government.

The Government and Contractor shall revise the measurement approach to include OCONUS sites. Within 60 days of availability of empirical data for at least two OCONUS site pairs, data will be collected and analyzed to support establishing an agreed upon target for OCONUS latency and packet loss.

Data for this SLA will be collected only when the Network is available.

Measurement CONOPS:

SLAPC 107.2 is measured via the Network Management System's (NMS) CiscoWorks 2000 InternetNetworking Performance Monitor (IPM), which is installed at a Network Operation Center (NOC). IPM measures from one of the site-pairs inner routers to one of the other site-pairs inner routers.

IPM holds one collector for each combination of source inner router and target-site inner router for the site pair. The source inner router's response time reporter (RTR) issues an Internet Control Message Protocol (ICMP) "ping" to the target site's inner router every minute. IPM collects the measurements from the inner router every hour and stores them in the CiscoWorks IPM internal SQL Anywhere database.

A scheduled software script automatically running from the CiscoWorks server exports the data daily to the SLAPC Oracle database where the data is aggregated for SLAPC reporting. The reported latency/packet loss measurements reflect a round-trip latency time value. The value that is stored for packet loss is the number of 'pings' that fail in that hour, which will be a number between 0 and 60.

SLAPC Latency Target adjustment for DISN Performance:

- The DISN core (backbone) is allocated the following latency values per month:
  -- 15.00 ms for Regional site pairs
  -- 60.00 ms for CONUS site pairs
  -- 110.00 ms for East Coast to Hawaii site pairs
  -- 170.00 ms for OCONUS site pairs
- If the DISN core (backbone) performance during a month can be shown through documented evidence to exceed the above latency values, then the corresponding SLAPC Targets for that month shall be adjusted by the difference between the actual DISN core (backbone) latency and the above latency values.

SLAPC Packet Loss Target adjustment for DISN Performance:

- The DISN core (backbone) is allocated 0.030% packet loss per month.
- If the DISN core (backbone) performance during a month can be shown through documented evidence to exceed 0.030% packet loss per month, then the SLAPC Targets for that month shall be adjusted by the difference between the actual DISN core (backbone) packet loss and 0.030%.

Who: Contractor	**Frequency:** Monthly
Where: **User Population:** All Navy; All USMC (measured separately) **Sample Size:** 100 Navy and USMC Selected Site Pairs along with twenty (20) VSSD sites (distributed among Navy and USMC and agreed upon by Government and Contractor) **Sample Unit:** Site (Representative of Hawaii-across-CONUS, CONUS, regional, and VSSD sites) **Where Measured:** Measured at the inner router.	**How Measured (i.e., captured):** Automated tool **Measurement Formula:** <u>Latency:</u> Service Level Attained = Number of latency round trip measurements within the required time interval / Total number of latency round trip measurements Values are calculated separately for each category (i.e., VSSD, Regional, CONUS, East Coast to Hawaii). <u>Packet Loss:</u> Service Level Attained = Number of packet loss measurements within the required values / Total number of packet loss measurements Measurement attempts blocked by the actions of the security boundary (firewalls) will not be computed in this measurement. This is not meant to exclude any delays due to normal VPN processing. **Frequency of Measure:** Every minute and aggregated to one value per hour **Weighting (as applicable):** Equal weighting for all site pairs.

Aggregation of Data:		Performance data for sites that have not yet achieved Full Performance will be aggregated at the site level and shall meet the Regional or CONUS target latency to the associated server farm calculated at the site level. Performance data for sites that have achieved Full Performance will be aggregated at the user population level and the SLAPC targets will apply at the user population level.	
SLAPC Success Criteria		All targets must be met, to pass the SLAPC	
	Latency		
SLAPC Target	**Area**	**Time Interval**	**Service Level Attained**
	VSSD Sites (Server Farm to 10 sites*)	60.0 ms regionally + backhaul or 100 ms CONUS + backhaul	>= 95.00%
	Regional (Within 600 miles**)	<= 60.0 ms	>= 95.00%
	CONUS (Coast-Coast)	<= 100.0 ms	>= 95.00%
	East Coast to Hawaii (Oahu Site)	<= 140.0 ms	>= 95.00%
	OCONUS (Quantico to Japan)	<= 200 ms	>= 95.00%
	Packet Loss		
SLAPC Target	**Area**	**Rate**	**% Attained**
	Enterprise	< 0.50%	>= 95.00%
	VSSD Sites	< 1.50%	>= 95.00%
		*i.e., shortest available telecommunications path. **VSSD CONUS sites are homed to a NOC, generally, within 600 telecommunications miles. Backhaul latency is to their respective server farm.	

Performance Category: Voice and Video Quality of Service	**Increment 1 SLAPC: 107.3**

Performance Category Description: VTC and Voice-over-IP are dependent on WAN QoS, specifically latency, packet loss, and jitter. Jitter is particularly relevant to IP supported voice and video and are industry standard measures for VTC service level measurement. Jitter is defined as:

> **Jitter:** Variation in the IP packets arriving caused by NMCI network congestion, timing drift, or route change. Unsatisfactory levels cause clicks in audio and flicker in the video display. The measure is the variation from when a packet was expected to be received at a destination and when it was actually received.

These measurements will be provided for the agreed-to pairs of "from" – "to" NMCI sites, as stipulated for latency and packet loss in the NMCI Intranet SLA. The Government and Contractor will mutually agree to adjust the site pairs when/if required, with the intent to identify performance problems if sub-optimum service occurs.

All measurements are based on a 24 hours a day/7 days a week operation.

SLAPC Jitter Target adjustment for DISN Performance:

The DISN core (backbone) is allocated the following jitter values per month:

- 3.00 ms average for ≥ 97.00% attained
- 10.00 ms maximum for ≥ 99.80% attained

If the DISN core (backbone) performance during a month can be shown through documented evidence to exceed the above jitter values, then the corresponding SLAPC Targets for that month shall be adjusted by the difference between the actual jitter of the DISN core (backbone) and the above jitter values.

The Government and Contractor shall revise the measurement approach to include OCONUS sites. Within 60 days of availability of empirical data for at least two OCONUS site pairs, data will be collected and analyzed to support establishing an agreed upon target for OCONUS jitter and bit rate. In January 2005, the Government and Contractor will analyze the target and upon mutual agreement readjust the target if deemed necessary.

Who: Contractor	**Frequency:** Monthly
Where: **User Population:** All Navy; All USMC (measured separately) **Sample Size:** 20 Navy and USMC Selected Site Pairs (distributed among Navy and USMC and agreed upon by Government and Contractor) **Sample Unit:** Site (Representative of Hawaii-across-CONUS, CONUS, and regional) **Where Measured:** Measured at the inner router.	**How Measured (i.e., captured):** Automated tool **Measurement Formula:** Number of measurements successful within each of the SLAPC Target times / Total number of attempts Measurement attempts blocked by the actions of the security boundary (firewalls) will not be computed in this measurement. This is not meant to exclude any delays due to normal VPN processing. **Frequency of Measure:** Every 5 minutes **Weighting (as applicable):** Equal weighting for all site pairs.
SLAPC Success Criteria:	All targets must be met, to pass the SLAPC

<table>
<tr><td>Aggregation of Data:</td><td colspan="3">Performance data for sites that have not yet achieved Full Performance will be aggregated at the site level and the SLAPC targets will apply at the site level.

Performance data for sites that have achieved Full Performance will be aggregated at the user population level and the SLAPC targets will apply at the user population level.</td></tr>
<tr><td rowspan="3">SLAPC Target</td><td rowspan="3">Jitter</td><td>Rate</td><td>% Attained</td></tr>
<tr><td>10.0 ms average</td><td>>= 97.00%</td></tr>
<tr><td>30.0 ms maximum average</td><td>>= 99.80%</td></tr>
</table>

Appendix A to SLAPC 106
Navy and Marine Corps CND Detection and Reporting Category Matrix (DRCM)
JTF-CNO Incident Categories

(Derived from CJCS Manual 6510.01)

Category 1 (Unauthorized Privileged (Root/Administrator) Access) – (Serious)
Access gained to a system and the use of root or Administrator privileges

Category 2 (Unauthorized Limited (User) Access) – (Serious)
Access gained to a system and the use of any user's privileges

Category 3 (Unauthorized Unsuccessful Attempted Access) –
Repeated attempts to gain access as root or user on the same host, service, or system with a certain number of connections from the same source

Category 3.1 (Serious) if meets any of the following:
- a) aaSignificant foreign source
- b) bbInvolves a classified system
- c) More than 100 attempts at a connection
- d) More than 5 bases, posts, camps, or stations are affected

Category 3.2 (Significant) if meets any of the following:
- a) Involves 10 to 100 attempts at a connection
- b) More than 2 to 5 bases, posts, camps or stations are probed

Category 3.3 (Simple):
- a) Less than 10 connections from the same source
- b) Affects one base, post, camp, or station

Category 4 Denial of Service Information Attack –
Any action that preempts or degrades performance of a system or network affecting the mission, business, or function of a base, post, camp, or station; Joint Operational Facility (JOF), agency, or service command and control system

Category 4.1 (Serious) if meets any of the following:
- a) Involves a classified system or network
- b) Isolates a base, post, camp, station, or joint Operational Facility (e.g. COMBATANT COMMANDER, or Theaters of Operation) from a network portion or service command and control system.
- c) Isolates a network (e.g., adversely affects functional software applications) that provides support to mission critical entities including the following communities:
  - DoD intelligence
  - Special operations
  - Logistical
  - Financial
  - Personnel
  - Command and Control
  - Medical
  - Research & Development, and

- Attack Warning/Attack Assessment

d) Denies availability of system or data (e.g., becomes isolated from either of the following service providers):
   - NIPRNet
   - SIPRNet
   - Unclassified ATM
   - Classified ATM
   - GCCS
   - GSCS
   - DISN
   - DMS
   - DISN
   - DSCS
   - DSN
   - AUTODIN networks, or
   - MEGACENTERS

e) Denies availability of DII components:
   - Routers
   - Hubs, or
   - Other Switching equipment

f) Leads to loss of life

Category 4.2 (Significant) if meets the following:

a) Successful limited isolation of a base, post, camp, or station, Joint Operational Facility or service command and control system

Category 4.3 (Simple) if meets the following:

a) Unsuccessful attempt at a Denial of Service Attack

Category 5 Poor Security Practices –

Any observed poor security practice such as poor passwords, direct privileged logins, privileged access via unsecured means, etc…which are collected from network monitor systems or logs. This also pertains to poor physical security

Category 5.1 – (Serious) if meets the following:

a) Inadvertent disclosure and/or poor security practices on a classified system or which provides access to classified systems by uncleared persons.

Category 5.2 – (Significant) if meets the following:

a) Direct root login

Category 5.3 – (Simple) if meets the following:

a) All others

Category 6 Unauthorized Probe –

Any attempt to gather information about an Automated Information System (AIS) or its users on-line by scanning a site and accessing ports through operating system vulnerabilities

Category 6.1 (Serious) if meets any of the following:

a) Involves a classified system
b) More than 10,000 ports are accessed
c) More than 5 bases, posts, camps or stations are probed

Category 6.2 (Significant) if meets any of the following:

a) 100 to 10,000 ports are accessed
b) 2 to 5 bases, posts, camps or stations are probed

Category 6.3 (Simple):

a) Less than 100 ports are accessed
b) One site probed

Category 7 Malicious Logic –

Any self-replicating software that is viral in nature; disseminated by attaching to or mimicking authorized computer system files; or acts as a Trojan Horse, an Easter Egg, or a Logic Bomb and is not deleted or quarantined by host-based anti-virus software.

This is regardless of whether the anti-virus software is not installed; not properly operating; disabled; definition files not up-to-date; service is not running; or is otherwise unable to recognize the malicious logic for any reason, the malicious logic will be considered not detected

Category 7.1 – (Serious) if meets the following:

a) Base, post, camp, station or more

Category 7.2 – (Significant) if meets the following:

a) Isolates to an organization

Category 7.3 – (Simple) if meets the following:

a) Isolates to a single machine

Reporting Priorities

Priority 1 – all (Serious) categories –

- Initial telephonic response is expected as soon as possible
    - Standard is within 15 minutes of detection
- Written report (e-mail or message) is expected within 8 hours of the initial telephonic response
- Follow-on and final reports are anticipated when the situation dictates

Priority 2 – all (Significant) categories –

- Initial telephonic response is expected as soon as practical
    - Standard is within 2 hours of detection
- Written report (e-mail or message) is expected within 8 hours of the initial telephonic response
- Follow-on and final reports are anticipated when the situation dictates

Priority 3 – all (Simple) categories –

- Initial telephonic response is expected as soon as practical
    - Standard is within 1 day of detection
- Written report (e-mail or message) is expected within 8 hours of the initial telephonic response
- Follow-on and final reports are anticipated when the situation dictates